Mata Kuliah : Kriptograpi	Sifat : Tutup Buku
Kelompok : A11	Waktu :
Hari / Tanggal :	Dosen :

Soal 1

Plaintext : 45F2389A

Key : A

Enkripsi Plaintext diatas dengan menggunakan metode Block Cipher **ECB dan CBC (15 Point)**

Soal 2

Diketahui 16 SubKey Algoritma DES:

K_2 = 011110 011010 111011 011001 110110 111100 100111 100101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010
K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

Tentukan Ciphertext dari **Plaintext 1234ABCD** dengan menggunakan Algoritma DES ??**(25 Point)**

Soal 3 Pembentukan Kunci RSA

Diketahui dua buah bilangan Prima **p= 37 , q= 47** cari **Private Key dan Public key** menggunakan algoritma RSA.

(25 Point)

Soal 4

a. Jelaskan perbedaan antara Staganografi dengan Cryptografi?
b. Sisipkan Pesan KRIPTOUDINUS, pada citra RGB sebesar 10 x 10 pixel seperti yang ditampilkan pada table matrix dibawah ini.

Pixel RGB	1	2	3	4	5	6	7	8	9	10
1	220,120,020	126,026,080	220,120,021	126,026,081	220,120,022	126,026,082	220,120,023	126,026,083	220,120,024	126,026,084
2	223,123,023	122,126,107	223,123,024	122,126,108	223,123,025	122,126,109	223,123,026	122,126,110	223,123,027	122,126,111
3	225,222,020	100,200,070	225,222,021	100,200,071	225,222,022	100,200,072	225,222,023	100,200,073	225,222,024	100,200,074

4	220,120,021	126,026,081	220,120,022	126,026,082	220,120,023	126,026,083	220,120,024	126,026,084	220,120,025	126,026,085
5	223,123,024	122,126,108	223,123,025	122,126,109	223,123,026	122,126,110	223,123,027	122,126,111	223,123,028	122,126,112
6	225,222,021	100,200,071	225,222,022	100,200,072	225,222,023	100,200,073	225,222,024	100,200,074	225,222,025	100,200,075
7	220,120,022	126,026,082	220,120,023	126,026,083	220,120,024	126,026,084	220,120,025	126,026,085	220,120,026	126,026,086
8	223,123,025	122,126,109	223,123,026	122,126,110	223,123,027	122,126,111	223,123,028	122,126,112	223,123,029	122,126,113
9	225,222,022	100,200,072	225,222,023	100,200,073	225,222,024	100,200,074	225,222,025	100,200,075	225,222,026	100,200,076
10	220,120,023	126,026,083	220,120,024	126,026,084	220,120,025	126,026,085	220,120,026	126,026,086	220,120,027	126,026,087

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Kode ASCI

(20 Point)

Soal 5

a. Sebutkan dan Jelaskan dua cara Penandatanganan Berkas digital dengan mengenkripsi Pesan pada Digital Signature?

b. 5B Terdapat kelemahan Penandatanganan Berkas Digital dengan mengenkripsi pesan menggunakan Pubic Key pada Digital Signature,jelaskan bagaimana solusi penyelesaian permasalahan tersebut? (jelaskan secara singkat dan jelas)

(15 Point)

OOO SELAMAT MENGERJAKAN OOO